Juniper Networks **NetScreen-Hardware Security Client**

The Juniper Networks NetScreen-Hardware Security Client, combined with NetScreen-Security Manager, is Juniper's most cost effective security solution for the fixed telecommuter and small remote office. It can easily be deployed and managed in large deployments with Juniper Network's Rapid Deployment capabilities, eliminating expensive staging steps. Using the same operating system as all NetScreen firewall and VPN solutions, the NetScreen-Hardware Security Client is able to provide the same level of protection as is found at the central sites.

	Juniper Networks NetScreen-Hardware Security Client 5 User or Plus
Maximum Performance and Capacity[1]	
ScreenOS version support	ScreenOS 5.3
Firewall performance	50 Mbps
3DES performance	10 Mbps
Deep Inspection (DI) performance	50 Mbps
Concurrent sessions	1,000
New sessions/second	1,000
Policies	50
Interfaces	5 10/100 Base-T
Number of supported users	5 or unrestricted
Mode of Operation	
Layer 2 mode (transparent mode)[2]	No
Layer 3 mode (route and/or NAT mode)	Yes
NAT (Network Address Translation)	Yes
PAT (Port Address Translation)	Yes
MIP/VIP Grouping	Yes
Home/work zones	Yes
Policy-based NAT	Yes
Users supported	5 or unrestricted
IPSec pass thru in NAT mode	5 or unrestricted
Firewall	
Number of network attacks detected	31
Network attack detection	Yes
DoS and DDoS protections	Yes
TCP reassembly for fragmented packet protection	Yes
Malformed packet protections	Yes
Deep Inspection (DI) firewall	Yes
Protocol anomaly	Yes
Stateful protocol signatures	Yes
Deep Inspection (DI) signature packs (See table on page 2)	Yes
Content Inspection	Yes
Embedded antivirus	Yes
Embedded Anti-Spam	Yes
Malicious Web filtering	Up to 48 URLs
External Web filtering (Websense or SurfControl)	Yes
Integrated Web filtering	Yes
Brute force attack mitigation	Yes
Deep Inspection (DI) attack pattern obfuscation	Yes
SYN cookie	Yes
Zone-based IP spoofing	Yes
Anti phishing[3]	Yes
Spyware / Adware / Keylogger Protection[4]	Yes
PKI Support	
PKI certificate requests (PKCS 7 and PKCS 10)	Yes
Automated certificate enrollment (SCEP)	Yes
Online Certificate Status Protocol (OCSP)	Yes
Self Signed Certificates	Yes

	Juniper Networks NetScreen-Hardware Security Client 5 User or Plus
PKI Support	
Certificate Authorities Supported	
Verisign	Yes
Entrust	Yes
Microsoft	Yes
RSA Keon	Yes
iPlanet (Netscape)	Yes
Baltimore	Yes
DOD PKI	Yes
VPN	
Concurrent VPN tunnels	2
Tunnel interfaces	3
DES (56-bit), 3DES (168-bit) and AES encryption	Yes
MD-5 and SHA-1 authentication	Yes
Manual Key, IKE, PKI (X.509)	Yes
Perfect forward secrecy (DH Groups)	1,2,5
Prevent replay attack	Yes
Remote access VPN	Yes
L2TP within IPSec	Yes
Dead Peer Detection	Yes
IPSec NAT traversal	Yes
Redundant VPN gateways	Yes
VPN tunnel monitor	Yes
Antivirus/Anti-Spam	
Embedded Scan Engine	Yes
Embedded Anti-Spam	Yes
Antivirus signatures	> 80,000
Protocols	POP3, SMTP, HTTP, IMAP, FTP
HTTP Webmail only	Yes
Maximum AV Users	5 or 25
Automated Pattern file updates	Yes
Firewall and VPN User Authentication	
Built-in (internal) database - user limit	up to 100
3rd Party user authentication	RADIUS, RSA SecurID, and LDAP
XAUTH VPN authentication	Yes
Web-based authentication	Yes
Logging/Monitoring	
Syslog (multiple servers)	External, up to 4 servers
E-mail (2 addresses)	Yes
NetIQ WebTrends	External
SNMP (v1, v2)	Yes
Standard and custom MIB	Yes
Traceroute	Yes
At session start and end	Yes
Virtualization	
Virtual Routers (VRs)	2
802.1Q VLan Tagging	No

	Juniper Networks NetScreen-Hardware Security Client 5 User or Plus
Routing	
RIPv1/v2 dynamic routing	2 instances
Static routes	1,024
Source Based Routing, Source Interface Based Routing	Yes
Equal cost multi-path routing	Yes
High Availability (HA)	
LDAP and RADIUS server failover	Yes
VoIP	
H.323 ALG	Yes
SIP ALG	Yes
MGCP ALG	Yes
NAT for H.323/SIP	Yes
IP Address Assignment	
Static	Yes
DHCP, PPPoE client	Yes
Internal DHCP server	Yes
DHCP relay	Yes
Authentication	
RADIUS Start/Stop	Yes
System Management	
WebUI (HTTP and HTTPS)	Yes
Command Line Interface (console)	No
Command Line Interface (telnet)	Yes
Command Line Interface (SSH)	Yes, v1.5 and v2.0 compatible
NetScreen-Security Manager	Yes
All management via VPN tunnel on any interface	Yes
Rapid deployment	Yes
Administration	
Local administrators database	20
External administrator database	RADIUS/LDAP/SecurID
Restricted administrative networks	6
Root Admin, Admin, and Read Only user levels	Yes
Software upgrades	TFTP/WebUI/SCP/NSM
Configuration Roll-back	Yes
Traffic Management	
Guaranteed bandwidth	Yes
Maximum bandwidth	Yes
Ingress Traffic Policing	Yes
Priority-bandwidth utilization	Yes
DiffServ stamp	Yes
Dimensions and Power	
Dimensions (H/W/L)	1/8.25/5 inches
Weight	1.3 lbs.
Rack mountable	Yes, with separate kit
Power Supply (AC)	
90 to 264 VAC to power supply	12 VDC, 12 W

Certifications

Safety Certifications

UL, CUL, CSA (5XT only), CB

EMC Certifications

FCC class B, BSMI Class A, CE class B, C-Tick, VCCI class B

Environment

Operational temperature: 23° to 122° F, -5° to 50° C

Non-operational temperature: -4° to 158° F, -20° to 70° C

Humidity: 10 to 90 % non-condensing

MTBF (Telecordia standard)

NetScreen-HSC: 32.2 years

Ordering Information

Product		Part Number
Juniper Networks NetScreen-HSC (5 user)		
NetScreen-HSC	US power supply	NS-HSC-001
NetScreen-HSC	UK power supply	NS-HSC-003
NetScreen-HSC	Europe power supply	NS-HSC-005
NetScreen-HSC	Japan power supply	NS-HSC-007
Juniper Networks NetScreen-HSC Upgrades		
NetScreen-HSC Upgrade from 5-User to NetScreen-HSC Plus (Unrestricted user)		NS-HSC-PLU

Deep Inspection (DI) Signature Packs

This feature enhancement allows ScreenOS to support targeted DI signature pack optimized for your specific network deployment. You can now select the DI signature pack that improves threat prevention for your network environment to ensure detection accuracy and coverage.

Protection Type	Deployment Type	Defense type	Attack Type
Base	Branch Offices Small/Medium Businesses	Client/Server and worm protection	Selected set of critical signatures
Client	Remote/Branch Offices	Perimeter defense, compliance for hosts (desktops, etc)	Attacks in the server-to-client direction
Server	Small/Medium Businesses	Perimeter defense, compliance for server infrastructure	Attacks in the client-to-server direction
Worm Mitigation	Remote/Branch Offices of Large Enterprises	Most comprehen-sive defense against worm attacks	Worms, Trojans, backdoor attacks

(1) Performance and capacity provided are the measured maximums under ideal testing conditions. May vary by deployment and features enabled.
(2) The following features are not supported in Layer 2 (transparent mode): NAT, PAT, policy based NAT, virtual IP, mapped IP, OSPF, BGP, RIPv2, and IP address assignment. Transparent mode only works in trust/untrust mode.
(3) Can be done through "site blocking" via URL filtering - whether integrated or redirect, and "inbound email blocking" via anti-spam and/or Juniper-Kaspersky embedded AV for those platforms which support it
(4) Juniper-Kaspersky engine only.

Juniper® NETWORKS

CORPORATE HEADQUARTERS AND SALES HEADQUARTERS FOR NORTH AND SOUTH AMERICA
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888-JUNIPER (888-586-4737)
or 408-745-2000
Fax: 408-745-2100
www.juniper.net

EAST COAST OFFICE
Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978-589-5800
Fax: 978-589-0800

ASIA PACIFIC REGIONAL SALES HEADQUARTERS
Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, Asia Pacific Finance Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA REGIONAL SALES HEADQUARTERS
Juniper Networks (UK) Limited
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U. K.
Phone: 44(0)-1372-385500
Fax: 44(0)-1372-385501

Copyright 2005, Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

110014-008 Nov 2005